面向蓝牙语音加密传输的波形码本设计

洪鹏程，黄一才，郁　滨

(信息工程大学，郑州 450001)

摘　要： 针对蓝牙语音信号加密后失去语音特征而不能通过语音信道传输的问题，建立蓝牙语音加密数据传输模型，提出一种面向蓝牙语音加密传输的波形码本生成算法。该算法以子载波调制生成初始调制码本，训练数据得到解调码本，通过设计末位淘汰机制的粒子对算法寻找最优码本。仿真分析表明，本文码本生成算法具有收敛速度快的优势，能够生成不同比特传输速率和符号错误率低的波形码本。实验结果表明，在蓝牙中使用该波形码本传输数据具有较低符号错误率。

关键词： 蓝牙；波形码本；波形符号；子载波调制；粒子对算法

中图分类号： TP309.1　　doi: 10.19734/j.issn.1001-3695.2018.10.0749

Waveform codebook design for Bluetooth voice encryption

Hong Pengcheng, Huang Yicai, Yu Bin

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Aiming at the problem that the Bluetooth voice signal cannot be transmitted through the voice channel after being encrypted, this paper establishes a Bluetooth voice encryption data transmission model, and proposes a waveform codebook generation algorithm for Bluetooth voice encryption transmission. The algorithm uses subcarrier modulation to generate the initial modulation codebook, and trains data to obtain the demodulation codebook. This paper designed the Particle-pair algorithm with the last elimination mechanism to find the optimal codebook. Simulation analysis shows that the proposed algorithm has the advantages of fast convergence rate and can generate waveform codebooks with different bit transmission rate and low symbol error rate. Experiments show that using this waveform codebook to transmit data in Bluetooth has low symbol error rate.

Key words: Bluetooth; waveform codebook; waveform symbol; subcarrier modulation; particle-pair algorithm

0　引言

蓝牙是一种短距离无线通信技术，已经成为手机、电脑等智能设备的标配，能够使蓝牙终端设备方便地与不同型号的手机连接并拨打免提电话。针对移动语音通信存在的安全问题[1]，在蓝牙终端设备中实现对语音加密传输是一种安全可靠的解决方案。

蓝牙与移动通信网均存在数据和语音两种信道，其数据信道传输语音难以达到实时性要求，而语音信道均使用了语音编解码器。蓝牙语音采用连续可变斜率增量调制（continuous variable slope delta modulation，CVSD）[2]，每个采样值仅采用 1 bit 量化；移动通信网使用有损的、有记忆的压缩编解码器[3]，且增加了语音激活检测（voice activity detection，VAD），这两种编解码器均不能传输不具备语音特征的加密语音信号。

目前国内外学者主要对在移动通信网语音信道上传输任意数据进行了深入研究，其核心思想是将数据转换成类语音后在语音信道上传输，具体又可分为语音合成、频率调制和波形码本三类[16]。

语音合成方案是将数据映射成语音特征参数合成类语音，文献[4,5]将数据映射成基音频率、线性频谱对和帧能量，文献[6]基于共振峰模型设计映射关系，但这类方案参数提取复杂，在嵌入式系统中难以达到实时性要求。在使用频率调制方案中，文献[7]提出的启发调制算法传输速率较低，文献[8~10]基于正交频分复用技术（orthogonal frequency division multiplexing，OFDM），将数据映射到语音频段的子载波生成类语音，但将其应用到蓝牙终端设备时，调制波形多次经过编解码器后出现较大扭曲，解调错误率较高。

相比前两种方案性能，波形码本方案具有计算量小和存储空间小的特点，波形码本能够实现“数据—符号—数据”传输，并由初始码本经遗传算法优化得到[11,12]。文献[13,14]直接选取人类语音筛选得到最优码本，但文献[11~14]均是仅针对指定的某种声码器设计码本。文献[15]建立波形符号在信道传输前后的平均欧氏距离分布概率模型，以此根据空间模型生成波形码本，实现了数据在声码器上的传输，但该方法忽视了声码器的自动幅值调节特性，使得欧氏距离出现偏差影响解调。文献[16]使用模式搜索算法设计码本，将数据映射在码本上后可以在多种不同声码器上传输，但是方案没有考虑蓝牙语音编解码的影响，不能直接应用到蓝牙终端。

与遗传算法、模式搜索等优化算法相比，粒子群算法具有实现简单、收敛速度快和受所求问题维度影响较小等特点[17]。纪震[17]在粒子群基础上设计了种群规模为 2 的粒子对算法，该算法在图像码书更新、基因聚类等应用中表现良好，在求解高维复杂问题上表现出了特别的优势。

收稿日期： 2018-10-09；**修回日期：** 2018-11-27

作者简介： 洪鹏程（1994-），男，湖南常德人，硕士研究生，主要研究方向为蓝牙、信息安全技术（hongpengcheng94@163.com）；黄一才（1985-），男，讲师，硕士，主要研究方向为蓝牙、信息安全技术；郁滨（1964-），男，教授，博导，博士，主要研究方向为信息安全、无线网络安全技术、视觉密码等.

综上所述，码本设计是使用码本传输蓝牙加密语音信号的关键，本文提出一种面向蓝牙语音加密传输的波形码本生成算法。该算法以子载波调制生成类语音作为初始调制码本，通过设计末位淘汰机制的粒子对算法，寻找能通过语音信道且符号错误率低的波形码本。

1 模型建立

为方便描述，本文相关符号及其含义如表 1 所示。

1.1 相关定义

定义 1 波形符号指包含 L 个采样值的类语音片段，用 $S=\{s_0,s_1,\cdots,s_{(L-1)}\}$ 表示。

定义 2 调制码本指与数据集 $\{0,1,2,\cdots,N-1\}$ 一一对应的波形符号集 $\{S_0,S_1,\cdots,S_{N-1}\}$，用 CA 表示，在发送语音时用于实现类语音调制。

定义 3 解调码本指调制码本 CA 中的每个波形符号 S_i $(0\le i\le N-1)$ 经过大量随机数据在语音信道传输后，接收端对应波形符号的所有输出平均值组成的集合 $\{SO_0,SO_1\cdots SO_{N-1}\}$，用 CB 表示。

波形码本包括调制码本和解调码本。

定义 4 比特传输速率指使用波形码本在语音信道每秒能够传输的比特数，用 R 表示。

定义 5 符号错误率指经过语音信道传输后解调错误波形符号数占总传输波形符号数的比例，用 SER 表示。

定义 6 最优码本指用于传输数据时优化能得到的符号错误率最低的波形码本。

定义 7 子载波指被调制用来传输信号、有固定频率的正/余弦波。

表 1 符号及含义

Table 1 Symbol and meaning

符号	含义	符号	含义
CA	调制码本	CB	解调码本
n	码本表示的比特数	N	码本中波形符号数量
L	波形符号采样点数	M	子载波频率数量
SER	符号错误率	S	波形符号
s	经语音信道传输后的波形符号	SO	接收波形符号的均值
R	比特传输速率	f_s	语音采样率
E	求均值	Δf	子载波频率间隔

1.2 数据传输模型

根据蓝牙终端语音数据传输过程，建立数据传输模型如图 1 所示，包括数据发送、数据传输和数据接收三个阶段。因模型传输对象是二进制码流，取 $N=2^n$（n 为整数）方便 CA 与比特流建立映射关系。

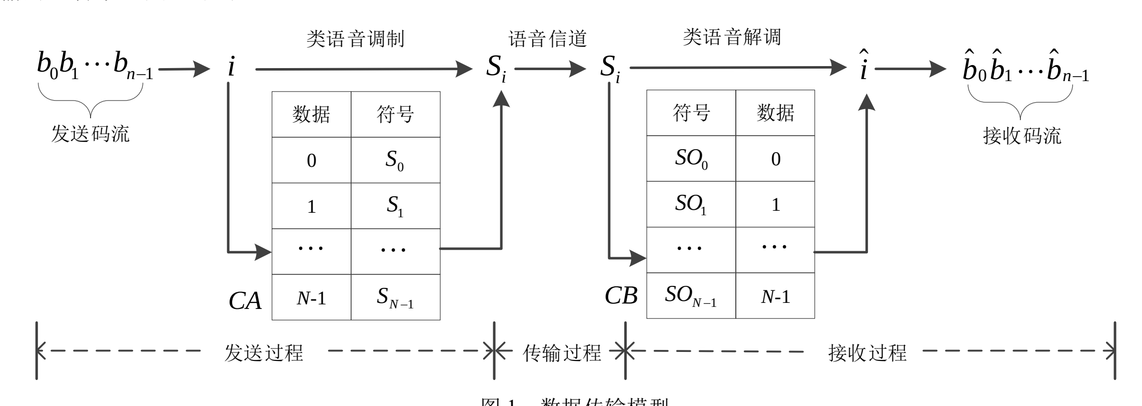


图 1 数据传输模型

Fig. 1 Data transmission model

在发送数据时，将分好组的二进制转换成数据 i，然后映射成对应的波形符号，即 $i\to S_i(0\le i\le N-1)$，最后将不同组的波形符号按序拼接成连续类语音 $[S_{i_1}^1,S_{i_2}^2,\cdots S_{i_k}^k\cdots]$ 发送。其中：$k\ge 1$，表示符号的发送序号；i_k 表示符号在码本中的序号。

依据数据传输模型，波形符号 $S_{i_k}^k$ 经语音信道传输后的波形为 $s_{i_k}^k$，其值主要由 $S_{i_k}^k$ 决定，但在 $S_{i_k}^k$ 之前传输的波形符号 $\{S_{i_1}^1,S_{i_2}^2\cdots S_{i_{k-1}}^{k-1}\}$ 也会使得波形 $s_{i_k}^k$ 波形出现不同程度的差异。因此，收方直接使用 CA 与 $s_{i_k}^k$ 进行比对判决发送的波形并不能达到最好效果。

基于此，为提高解调成功率，使用解调码本 CB 与接收波形 s_i 比对来判决发送的波形，以实现 $s\to SO_i\to\hat{i}$ $(0\le i\le N-1)$。判决方法是通过求接收的波形符号 s_i^k 与符号集合 $\{SO_i\}$ 的余弦值来实现匹配，余弦值越大，说明两个波形相似度越高，将余弦值最大的对应波形解调为发送的波形，再还原出发送的数据，即 $\hat{i}=\arg\max_i[\cos(SO_i,s_i^k)]$。

评价一个波形码本的指标包括比特传输速率、计算量、存储量和符号错误率。其中，前三个指标由码本规模决定。本文对规模设定为 $N\times L$ 的码本生成与优化，即在码本规模确定时得出符号错误率低的波形码本。此外，还研究了码本规模对符号错误率的影响。

2 波形码本生成算法

以子载波调制生成类语音波形组成初始调制码本，训练数据生成解调码本，通过设计粒子编码、优化目标函数和粒子更新机制，使用末位淘汰机制的粒子对算法寻找最优码本。

2.1 码本初始化

2.1.1 调制码本初始化

为使波形符号满足语音频段要求（$[f_{\min},f_{\max}]=[300Hz,3400Hz]$），使用子载波调制生成类语音作为波形符号。在 $[f_{\min},f_{\max}]$ 频率范围内，以 Δf 为相等频率间隔设置子载波频率值，则共需要子载波频率值的数量 M 为

$$M=\left\lfloor\frac{f_{\max}-f_{\min}}{\Delta f}\right\rfloor+1$$

其中每个频率值分别对应一个正弦和余弦子载波。

波形符号 S_i $(0\le i\le N-1)$ 初始生成流程如下。

a) 随机生成子载波幅值 G_i：

$$G_i=\{z_{i0},z_{i1},\cdots,z_{i(2M-2)},z_{i(2M-1)}\}$$

其中：z_{ij} $(0\le i\le N-1,0\le j\le 2M-1)$ 是从 $[-1,1]$ 区间的随机数，当

j 为偶数和奇数时 z_{ij} 分别对应正弦和余弦子载波的幅值，则由子载波调制得到的类语音波形时域表达式 $f_i(t)$ 为

$$f_i(t)=\begin{cases} z_{i0}\sin(2\pi f_{\min}t)+z_{i1}\cos(2\pi f_{\min}t)+ \\ z_{i2}\sin(2\pi(f_{\min}+\Delta f)t)+z_{i3}\cos(2\pi(f_{\min}+\Delta f)t)+ \\ \cdots \\ z_{i(2M-4)}\sin(2\pi(f_{\min}+(M-2)\Delta f)t)+z_{i(2M-3)}\cos(2\pi(f_{\min}+(M-2)\Delta f)t)+ \\ z_{i(2M-2)}\sin(2\pi(f_{\min}+(M-1)\Delta f)t)+z_{i(2M-1)}\cos(2\pi(f_{\min}+(M-1)\Delta f)t) \end{cases}$$

b) 以语音采样率 f_s 对 $f_i(t)$ 从 $t=0$ 时开始采样，取前 L 个采样值作为 S 。

c) 功率归一化， $S=\frac{S}{|S|}$ ， $|S|$ 表示向量的模，即得到一个采样点数为 L 的波形符号，结束。

为使每个波形符号的功率一致，在得到波形符号后，需要对其功率进行归一化运算。

对波形符号的初始生成过程进行分析可知：a)子载波幅值 $G=\{z_0,z_1,\cdots,z_{(2M-2)},z_{(2M-1)}\}$ 决定了波形符号 S ；b)随机生成子载波幅值，生成的波形符号满足语音频段要求；c)随机生成 N 组子载波幅值，可以得到 N 个波形符号组成初始调制码本 CA；d)最终得到波形符号 S 的采样值位于[-1,1]间，在使用时需要将其转换成蓝牙支持的 16 bit 位宽。

2.1.2 解调码本初始化

通过初始调制码本 CA 在语音信道传输大量随机数据，从而训练得到初始解调码本 CB。将数据需要透传的声码器用 $Vocoder_1,Vocoder_2,\cdots,Vocoder_H$ 表示。因此数据经历的编解码组合为 $CVSD$+$Vocoder_1$、$CVSD$+$Vocoder_2$、…、$CVSD$+$Vocoder_H$ 等 H 种。

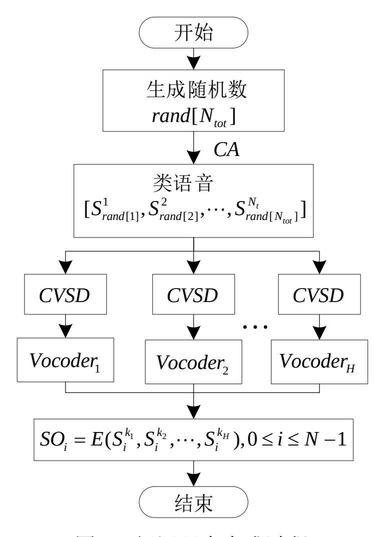


图 2　解调码本生成过程

Fig. 2　Generation process of demodulation codebook

解调码本生成过程如图 2 所示。首先生成 N_{tot} 个 $[0,N-1]$ 之间的随机数，利用 CA 映射成波形符号并组合成连续的类语音，分别在 H 个编解码组合中传输；然后求解 $S_i(0\le i\le N-1)$ 经每种组合传输后的所有输出值平均值作为 SO_i ，进而得到 CB。

2.2　码本优化

由 2.1 节分析可知，如图 3 所示，生成子载波幅值即可得到相应的调制码本和解调码本，进而可以计算码本的 SER。因此，问题转换为求使得 SER 最低的子载波幅值，具体如下。

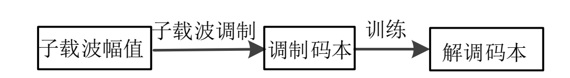


图 3　码本生成过程

Fig. 3　Generation process of codebook

2.2.1 粒子编码

在优化过程中，使用每个粒子表示一个调制码本，故需将一个调制码本中所有波形符号的子载波幅值 G_0、G_1、…、G_{N-1} 作为一个粒子的编码。

因此，将 N 组子载波幅值 G_0、G_1、…、G_{N-1} 按序排列可得到粒子编码，记为 $Z=(z_{00},z_{01},\cdots,z_{(N-1)(2M-1)})$ ，且 Z 是一个 $2MN$ 维向量，如表 2 所示。

表 2　粒子编码

Table 2　Particle coding

$z_{00},z_{01},\cdots,z_{0(2M-1)}$	$z_{10},z_{11},\cdots,z_{1(2M-1)}$	$\cdots$	$z_{(N-1)0},z_{(N-1)1},\cdots,z_{(N-1)(2M-1)}$

因为子载波幅值设定位于[-1,1]区间，粒子初始化时只需要从[-1,1]区间生成 $2MN$ 个随机数作为 $Z=(z_{00},z_{01},\cdots,z_{(N-1)(2M-1)})$ ，而且该初始粒子对应一个初始调制码本。

2.2.2 目标函数

判断粒子优劣时，先得到对应的解调码本。然后使用调制码本在 H 个不同编解码组合传输 N_{total} 个 $[0,N-1]$ 之间的随机数，通过解调码本得到在不同组合中的解调错误数 $N_{err_1},\cdots,N_{err_H}$ ，计算其 SER 均值作为目标函数。

$$D=\overline{SER}=\frac{1}{H}\sum_{j=1}^{H}\frac{N_{err_j}}{N_{total}}$$

D 值越小,粒子性能越好。

2.2.3 粒子更新机制

优化算法包含两对独立的粒子对 $\{Z_1^{(k)},Z_2^{(k)}\}$ 和 $\{Z_3^{(k)},Z_4^{(k)}\}$ ，其中 k 表示粒子迭代次数。每次迭代过程中，每对粒子按如下操作更新：

按照 $V_t^{k+1}=\omega V_t^k+c_1r_1(p_t-Z_t^k)+c_2r_2(p_g-Z_t^k)$ 更新速度，按照 $Z_t^{k+1}=Z_t^k+V_t^{k+1}$ 更新位置。其中： r_1 与 r_2 为[0,1]之间的随机数； c_1 和 c_2 是学习因子； ω 是权重因子。设定粒子位置边界为[-1,1]，速度边界 $[v_{\min},v_{\max}]$ 。

为使粒子有更好的搜索能力，对性能较差粒子对应调制码本中的波形符号进行末位淘汰并重新生成。具体实现过程如下：首先计算两个粒子目标函数值，取目标函数值较大者对应的粒子；然后计算该粒子对应码本的每个波形符号在 H 个编解码组合中的 SER 均值，即

$$f(i)=\frac{1}{H}\sum_{j=1}^{H}\frac{N_{err_j}(i)}{N_{total}(i)},0\le i\le N-1$$

将 $f(i)$ 最大值对应的波形符号判别为效果不好的波形符号 S_q ：最后随机生成一个新的子载波幅值，将子载波幅值 $G_{S_q}=(z^t_{S_q0},z^t_{S_q0},\cdots,z^t_{S_q(2M-1)})$ 在粒子相应位置替换。

按上述更新机制， $\{Z_1^{(k)},Z_2^{(k)}\}$ 和 $\{Z_3^{(k)},Z_4^{(k)}\}$ 分别按照粒子群算法最多迭代 $N_{\max}$ 次后，将 D 较低粒子重新组成精英粒子对 $\{Z_5^{(k)},Z_6^{(k)}\}$ ，继续迭代最多 $N_{\max_2}$ 次得到最优粒子 Z_7 ，将 Z_7 对应码本作为最优解调码本。

2.2.4 码本优化算法流程

引入末位淘汰机制的粒子对算法对码本进行优化，其流程如图 4 所示。

具体流程如下，其中 $p_t^{(k)}$ 保存当次迭代最优粒子， $p_g^{(k)}$ 保存自迭代以来全局最优的粒子。

a)设置 $j=1$ ， $t_1=1$ ， $t_2=2$ ，设置阈值 ε 和最大迭代次数 $N_{\max}$ 。

b) 设置 $k=0$ ，初始化粒子位置和速度， $Z_t^{(k)}=(z^t_{00},z^t_{01},\cdots,z^t_{(N-1)(2M-1)})$ 、 $V_t^{(k)}=(v^t_{00},v^t_{01},\cdots,v^t_{(N-1)(2M-1)})$ ，其中 $t=t_1,t_2$ 。

c)粒子 $Z_t^{(k)}$ 运算得到调制码本 $CA_t^{(k)}$ 。

d)将 N_{tot} 个 $[0,N-1]$ 之间的随机数映射到 $CA_t^{(k)}$ 上在语音信道传输，训练生成解调码本 $CB_t^{(k)}$ 。

e)将 N_{total} 个 $[0,N-1]$ 之间的随机数映射到 $CA_t^{(k)}$ 上在语音信道传输，并使用 $CB_t^{(k)}$ 解调。

f)计算每个粒子 $Z_t^{(k)}$ 的目标函数值 $D_t^{(k)}$ ，计算 $D^{(k)}=\min\{D_1^{(k)},D_2^{(k)}\}$ ，将 $D^{(k)}$ 其对应粒子作为局部最优粒子 $p_t^{(k)}$，将至今目标函数值最好粒子作为全局最优粒子 $p_g^{(k)}$ 。

g)若 $D^{(k)}<\varepsilon$，结束。

h)设置 $k=k+1$ ，更新粒子速度和位置，$V_t^{k+1}=\omega V_t^k+c_1r_1(p_t-Z_t^k)+c_2r_2(p_g-Z_t^k)$ 、 $Z_t^{k+1}=Z_t^k+V_t^{k+1}$ 。

i)若 $D_{t_1}^{(k-1)}>D_{t_2}^{(k-1)}$ ，计算得出 $Z_{t_1}^{k-1}$ 中解调错误率最高符号 S_{q_1} ，重新随机生成粒子 $Z_{t_1}^k$ 中子载波幅值 $G_{q_1}=(z_{S_{q_1}0}^{t_1},z_{S_{q_1}1}^{t_1},\cdots,z_{S_{q_1}(2M-1)}^{t_1})$ ；否则计算得出 $Z_{t_2}^{k-1}$ 中解调错误率最高符号 S_{q_2} ，重新随机生成粒子 $Z_{t_2}^k$ 中子载波幅值 $G_{q_2}=(z_{S_{q_2}0}^{t_2},z_{S_{q_1}0}^{t_2},\cdots,z_{S_{q_2}(2M-1)}^{t_2})$ 。

j)若 $k<N_{\max}$ ，跳至步骤 c)； $\{Z_5,Z_6\}$

k)得到较优粒子 $Z_{j+4}=p_g^{(k)}(j=1,2,3)$ ， $j=j+1$， 若 $j=2$ ，则跳至步骤 b)，$t_1=3,t_2=4$；若 $j=3$，则设置初始种群为 $t=5,6$，设置 $N_{\max}=N_{\max 2}$ ，跳至步骤 c)；若 $j=4$，结束。

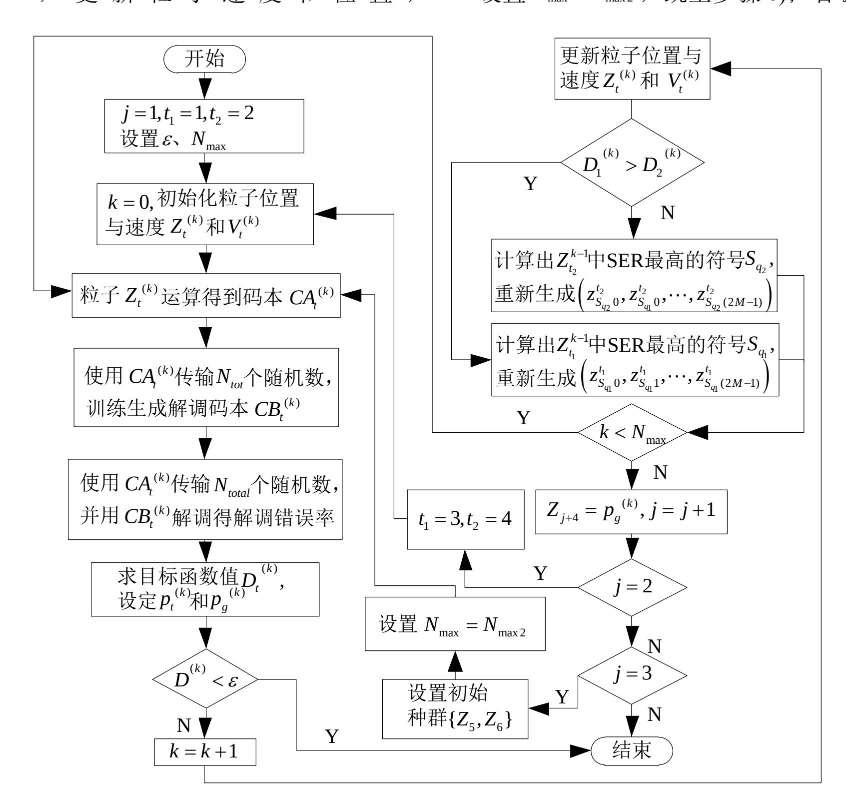


图 4　码本优化流程

Fig. 4　Codebook optimization flow chart

3　波形码本生成算法

首先在仿真环境中使用本文算法生成波形码本，其中 CVSD 和声码器分别按照蓝牙技术联盟和欧洲电信标准化协会所制定的标准实现，然后对波形码本的各指标分析，最后通过手机通话检验码本在蓝牙中应用效果。

3.1　实验设置

移动通信网使用 FR、EFR、HR 和 AMR 等多种声码器，前三种用于 2G 的 GSM 通信，第四种用于 3G/4G 通信。采用本文算法选取 CVSD 分别和 EFR、FR、AMR12.2、AMR10.2 和 AMR7.95 五种声码器组合对码本优化，并得到不同规模码本。在波形码本生成算法中，$\Delta f=50Hz$ ，$N_{\max}=5000$ ，$N_{\max 2}=2000$ ，N_{tot} 和 N_{total} 均为 10^5，$\varepsilon=10^{-5}$ ，c_1 和 c_2 分别为 0.3 和 0.5，码本范围 C_i 范围为[-1,1]，粒子最大速度 v_i 取值为[-0.1,0.1]，权值 ω 取 0.1。

在实际验证阶段，使用两部小米手机 6 和两个 CSR8670 蓝牙开发平台对码本传输性能进行测试，测试环境如图 5 所示。



图 5　实测示意图

Fig. 5　Schematic diagram in practical testing

3.2　结果分析

码本指标部分结果如表 3 所示。其中计算量指对接收波形解调时求解余弦值的运算量，约为 8 000 N 次/s 加法和乘法；存储量指 $CA_{N\times L}$ 和 $CB_{N\times L}$ 占用空间，为 $2LN$。

由表 3 可以看出，相同码本在不同组合中的 SER 不一样，其中码本在 CVSD+EFR 和 CVSD+AMR12.2 两种组合中传输效果较好，而在 CVSD+FR 组合中的传输效果较差。

图 6 表示在码本中波形符号数量 N 相同情况下，SER 与波形符号长度 L 的关系。波形符号长度 L 越长，SER 越低，即 $SER\propto\frac{1}{L}$ 。

表 3　算法性能

Table 3　Algorithm performance

码本规模		32x40	64x40	32x30	64x36	32x20	64x24	64x20
R（kb/s）		1	1.2	1.33	1.33	2	2	2.4
SER (%)	EFR	0.004	0.013	0.008	0.007	0.056	0.048	0.264
	FR	0.351	0.897	1.798	1.542	4.325	4.214	12.507
	AMR12.2	0.002	0.013	0.007	0.006	0.049	0.041	0.278
	AMR10.2	0.051	0.092	0.054	0.045	1.218	1.104	3.479
	AMR7.95	0.956	3.478	5.914	4.813	7.547	6.957	15.995
计算量（10^3 次/秒）		256	512	256	512	256	512	512
存储量（双字）		2560	5120	960	2304	640	1536	1280

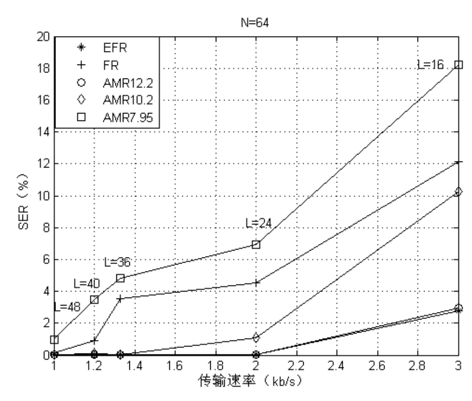


图 6　*L* 不同时的 *SER*

Fig. 6　*SER* with different *L*

图 7 表示在码本中波形符号长度 L 相同情况下，SER 与波形符号数量 N 的关系。符号数量 N 越小，SER 越低，即 $SER \propto N$ 。

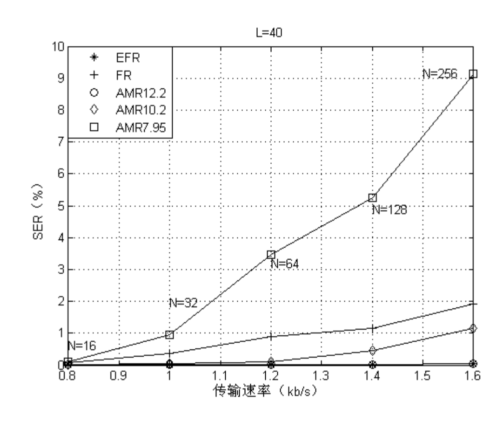


图 7　*N* 不同时的 *SER*

Fig. 7　*SER* with different *N*

图 8 表示在 *R* 相同的情况下，不同 *N* 和 *L* 组合的 *SER*。由图 8 可知，波形符号的采样点数 *L* 越多，*SER* 也越低。但是随着 *L* 增大，*N* 呈指数级增大，计算量和存储量也随之迅速上升；同时，寻找 *N* 个既具有差异性又能通过语音信道的波形符号的难度会越大，*SER* 降低比例会越来越小。因此，在考虑既定比特传输速率的码本时，需对 *SER*、存储量和计算量折中考虑。

图 9 表示对规模为 32×20 的码本优化时，CVSD+EFR 组合的 *SER* 与迭代次数关系。其中，对初始粒子迭代 5 000 次，对精英粒子迭代 2 000 次，每次迭代对两个粒子搜寻，总搜寻次数为 24 000 次。

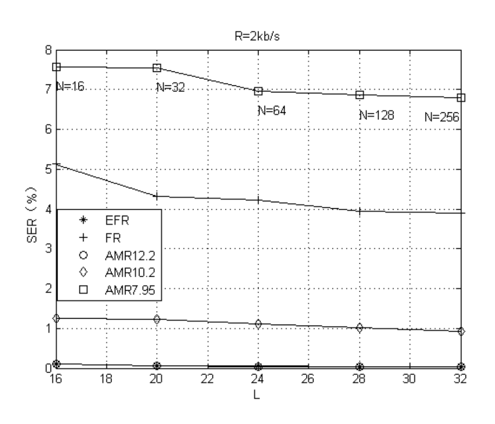


图 8　相同 *R* 时的 *SER*

Fig. 8　SER in same R

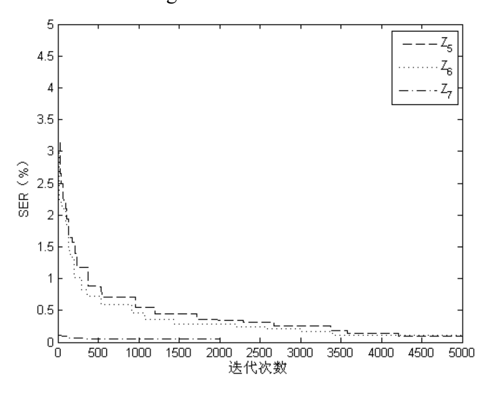


图 9　迭代时的 *SER*

Fig. 9　*SER* in Iteration

表 4 为文献[16]与本文算法对比。其中文献[16]使用模式搜索算法优化，其实际搜寻次数为迭代次数 8 000 次与每次迭代寻找方向 1 024 之积，即 8 192 000 次。文献[16]整体上 *SER* 低于本文算法，但是并没有考虑 CVSD，而且运算量大，整体上本文算法性能较优。

表 4　性能对比

Table 4　Performance comparison

	SER	CVSD 编解码	总搜寻次数
文献[16]	0.0004%	未考虑	8192000
本文	0.056%	考虑	24000

表 5 表示利用本文算法生成的码本在 CVSD 和不同声码器组合中所能承载的最大比特传输速率，其中 *SER* 在 5%内时认为可以通过纠错码纠正。

表 5　不同声码器最大的比特传输速率

Table 5　Maximum bit rate of different vocoders

声码器	EFR	FR	AMR12.2	AMR10.2	AMR7.95
R_{max}（kb/s）	3	2	3	2.4	1.33

手机可以设置语音通话的网络，但不能指定声码器，因此在实测时，先将波形码本烧入到 CSR8670，然后分别指定 2G、3G/4G 网络进行语音通话，每次通话循环发送 1 000 个波形符号，在接收方提取接收数据在 MATLAB 中实现同步后再解调，计算其 *SER*，做 10 次实验取其平均值，*SER* 结果如表 6 所示。

由表 6 可知，实测实验结果比仿真测试要差，原因有：a)语音传输会受到更多因素的影响，如电磁干扰，信号衰减等；b)移动通信网的语音通信会在不同声码器之间切换，如 2G 可能使用 EFR、FR 和 HR 等声码器，而 3G/4G 网使用的 AMR 声码器会根据信道采用不同编码速率，但是符号错误率仍在可接受范围内，通过纠错码传输可以较好地解决。

表 6 测试结果

Table 6 Test results

网络类型	码本规模				
	32x40	64x40	64x36	64x24	64x20
2G	0.02%	0.32%	0.54%	1.58%	1.78%
3/4G	0.12%	0.33%	0.22%	1.83%	1.34%

4 结束语

本文在深入分析 CVSD 编码和声码器特点的基础上，提出了一种面向蓝牙语音加密传输的波形码本生成算法。该算法使用固定频率在语音频段的子载波调制生成初始调制码本，在语音信道训练数据得到解调码本，设计了粒子编码、优化目标函数和粒子更新机制，使用末位淘汰机制的粒子对算法寻优。仿真分析表明，算法收敛速度快，可以生成不同比特传输速率和符号错误率低的波形码本。在此基础上，设计了实验用于检验波形码本在蓝牙设备中传输数据效果，结果表明符号错误率较低。下一步需要继续实现蓝牙语音加密数据自同步，进而实现蓝牙语音加密数据在语音信道透传。

参考文献：

[1] 韩心梓. 移动通信端到端语音加密传输技术研究 [D]. 南京：东南大学, 2016. (Han Xinzi. Research on end-to-end voice encryption and transmission technology for mobile communication [D]. Nanajing:Southeast University, 2016.)

[2] Bluetooth SIG, Bluetooth SIG specification of the Bluetooth system: core package version 5. 00 [EB/OL]. (2016) [2018-09-01]. http: www. bluetooth. org.

[3] European Telecommunications Standards Institute. Digital cellular telecommunications system (Phase 2) (200) enhanced full rate (EFR) speech transcoding (GSM 06. 60 version 4. 1. 1) [EB/OL]. (2000) [2018-09-01]. http://www. etsi. org.

[4] Kaiugampala N, Villette S, Kondoz A M. Secure voice over GSM and other low bit rate systems [C]// Proc of IEEE Seminar on Secure Gsm & Beyond: End to End Security for Mobile Communications. London: IEEE Press, 2003: 3/1-3/4.

[5] 杨典兵. 端到端保密通信中的类语音调制解调研究 [D].郑州：信息工程大学, 2009. (Yang Dianbing. Research on speech-like modulation and demodulation in end-to-end secure communication [D]. Zhengzhou:Information Engineering University, 2009.)

[6] Rashidi M, Sayadiyan A, Mowlaee P. Data mapping onto speech-like signal to transmission over the gsm voice channel [C]// Proc of the 40th Southeasten Symposium on System Theory.New Orleans: IEEE Press, 2008: 54-58.

[7] Sapozhnykov D A, Sharma A, Paik M, *et al.* Hermes: data transmission over unknown voice channels [C]// Proc of International Conference on Mobile Computing and Networking.Chicago: DBLP, 2010: 113-124.

[8] Chen L, Guo Q. An OFDM-based secure data communicating scheme in GSM voice channel [C]// Proc of International Conference on Electronics, Communications and Control. Ningbo: IEEE Press, 2011: 723-726.

[9] 唐旭. 数字信号在语音信道中的传输算法研究 [D]. 西安：西安电子科技大学, 2014. (Tang Xu. Research on algorithm of digital signal transmission in speech channel [D]. Xi·an:Xidian University, 2014.)

[10] 杨于村. 基于公众移动通信网的端到端加密语音传输技术研究 [D]. 广州：华南理工大学, 2009. (Yang Yucun. Research on transmission technology for end-to-end encrypted voice over public mobile networks [D]. Guangzhou:South China University of Technology, 2009.)

[11] Ladue C K, Sapozhnykov V V, Fienberg K S. A data modem for GSM voice channel [J]. IEEE Trans on Vehicular Technology, 2008, 57 (4): 2205-2218.

[12] 梁丹, 张连海, 杨绪魁. 一种新型的类语音调制方法 [J]. 电子设计工程, 2017, 25 (4): 5-10. (Lian Dan, Zhang Lianhai, Yang Xukui. A new method of speech-like modulation [J]. Electronic Design Engineering, 2017, 25 (4): 5-10.)

[13] Boloursaz M, Hadavi A H, Kazemi R, *et al.* A data modem for GSM adaptive multi rate voice channel [C]// Proc of East-West Design & Test Symposium.Rostov-on-Don: IEEE Press, 2013: 1-4.

[14] 梁丹, 陈琦, 张连海. 一种基于遗传算法的类语音调制方法 [J]. 信息工程大学学报, 2017, 18 (2): 148-153. (Lian Dan, Cheng Qi, Zhang Lianhai. Speech-like modulation method based on genetic algorithm [J]. Journal of Information Engineering University, 2017, 18 (2): 148-153.)

[15] Kazemi R, Boloursaz M M, Heidari K M, *et al.* Modem based on sphere packing techniques in high-dimensional Euclidian sub-space for efficient data over voice communication through mobile voice channels [J]. Communications Iet, 2015, 9 (4): 508-516.

[16] Sapozhnykov V V. A Low-rate data transfer technique for compressed voice channels [J]. Journal of Signal Processing Systems, 2012, 68 (2): 151-170.

[17] 纪震. 粒子群算法及应用 [M]. 北京：科学出版社, 2009. (Ji Zhen. Particle swarm optimization algorithm and application [M]. Beijing:Science Press, 2009.)